

## UNITED STATES DISTRICT COURT

for the  
Northern District of New York

In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)

Accounts associated with Mark J. Wallace, Jr.,  
heavyfoot48@hotmail.com, heavyfoot48@gmail.com and/or  
screen name "Mark Wall" that are stored at the premises  
owned by Dropbox, Inc. in San Francisco, California, described

Case No. 5:17-MJ-272 (DEP)

in Attachment A **APPLICATION FOR A SEARCH WARRANT**

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):  
Dropbox Accounts Associated with Mark J. Wallace, Jr., heavyfoot48@hotmail.com, heavyfoot48@gmail.com and/or screen name "Mark Wall" that are stored at the premises owned by Dropbox, Inc. in San Francisco, California, described in Attach A

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☐ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
Title 18, U.S.C., Sections 2252A(a)(2)(A) & 2252A(a)(5) (B)	Receipt, Distribution and Possession of child pornography

The application is based on these facts:  
See attached Affidavit

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
 Applicant's signature  
 Lon Ziankoski, Special Agent  
 Printed name and title

Sworn to before me and signed in my presence.

Date: 06/09/2017

  
 Judge's signature

City and state: Syracuse, New York

Hon. David E. Peebles, U.S. Magistrate Judge  
 Printed name and title

**ATTACHMENT A**

**Property to be searched**

The property to be searched are the Dropbox accounts associated with Mark J. Wallace, Jr., heavyfoot48@hotmail.com, heavyfoot48@gmail.com and/or the screen name "Mark Wall" that are stored at premises owned, maintained, controlled, or operated by Dropbox, Inc., headquartered at 185 Berry Street, 4th Floor, San Francisco, CA 94107 (hereinafter, the "accounts").

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Dropbox, Inc.**

To the extent that the information described in Attachment A is within the possession, custody, or control of Dropbox, Inc. including any messages, records, files, images/videos, logs, contacts or information that have been deleted but are still available to Dropbox, Inc. or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Dropbox, Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all communications associated with the listed accounts, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
- b. All records or other information regarding the identification of the accounts, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the accounts were created, the length of service, the IP address used to register each account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;

d. All records or other information stored at any time by an individual using the accounts, including address books, contact and buddy lists, calendar data, pictures, documents and files;

e. All records pertaining to communications between Dropbox and any person regarding the account, including contacts with support services and records of actions taken; and

f. All connection logs and records of user activity for the account, including:

- i. Connection and date time;
- ii. Disconnect date and time;
- iii. Method of connection;
- iv. Data transfer volume;
- v. User name associated with the connection and other connection information, including the internet protocol address of the source of the connection; and
- vi. Connection information for other computers to which the user of the above-referenced accounts connected, by any means, during the connection period, including the destination IP address, connection time and date, disconnect time and date, method of connection to the destination computer, the identities (account and screen names) and subscriber information, if known, for any person or entity to which such connection information relates, and all other information related to the connection from ISP or its subsidiaries.

## **II. Information to be seized by the government**

All information described above in Section I that constitutes evidence and instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A (distribution, receipt and possession of child pornography), from January 1, 2014 to present, including, for each account or identifier listed on Attachment A:

- (a) Subscriber information, such as name, email address, zip code and other personal/biographical information;
- (b) Account access information, master and sub account names, user profiles, friends lists, instant messages, grief reports, account creation information, associated IP information for each account use, screen shots of account activity, email transaction information;
- (c) Computer records and evidence identifying who the particular user was who received, downloaded, possessed, or accessed with intent to view any child pornography found on any computer or computer media (evidence of attribution), or who attempted to do any of the foregoing, and how the computer was used to effectuate that activity;
- (d) Any and all visual depictions of minors, including, but not limited to, sexually explicit images of minors.
- (e) Any and all chats, chat logs, emails, and other text documents, describing or relating to sexually explicit conduct with children, as well as fantasy writings regarding, describing, or showing a sexual interest in children.

- (f) Any and all address books, names, and lists of names and addresses of minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18 United States Code, Section 2256(2).
- (g) Any and all notebooks and any other records reflecting personal contact, and any other activities, with minors who may be visually depicted while engaged in sexually explicit conduct, or engaged in sexually explicit chat, email, or other communications.
- (h) Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, notes, and sexual aids.

**AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT**

I, Lon Ziankoski, a Special Agent with Homeland Security Investigations, being duly sworn, depose and state as follows:

**INTRODUCTION**

1. I am a Special Agent assigned to Homeland Security Investigations (HSI) within the Department of Homeland Security and have been employed in that capacity since September 2011. I am currently assigned to the HSI office in Syracuse, New York where I am responsible for conducting investigations of criminal violations of immigration and customs laws and related statutes. As an HSI Special Agent my duties include the enforcement of federal criminal statutes involving child exploitation laws. I have worked closely with other law enforcement officers who have engaged in numerous investigations involving child exploitation and child pornography and who have received training in the area of child pornography and child exploitation. Since becoming employed as a federal agent, I have completed the Criminal Investigator Training Program and ICE Special Agent Training at the Federal Law Enforcement Training Center in Brunswick, Georgia. I have also received Internet Crimes Against Children (ICAC) certification in Undercover Chat Investigations. I have taught child exploitation investigations to foreign law enforcement agencies at the International Law Enforcement Academy in Gaborone, Botswana. Prior to appointment as an Agent, Affiant was employed as an Oswego County Sheriff's Deputy for approximately two years. I served honorably in the United States Army, 10th Mountain Division as a Non-Commissioned Officer with deployments in support of Operation Enduring Freedom and Operation Iraqi Freedom. Your affiant has earned a Bachelor's Degree in Biology from Rochester Institute of Technology, a Doctorate in Chiropractic from Palmer College, and a Master's in

Business Administration from Sul Ross Texas State University.

2. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

3. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored at premises owned, maintained, controlled, or operated by Dropbox, Inc., headquartered at 185 Berry Street, 4th Floor, San Francisco, CA 94107. Dropbox, Inc. provides an online storage medium on the internet accessed from a computer or electronic storage device. The Dropbox, Inc. accounts to be searched are Dropbox, Inc accounts associated with Mark J. Wallace, Jr., heavyfoot48@gmail.com, heavyfoot48@hotmail.com, and/or the screen name "Mark Wall" further described in the following paragraphs and in Attachment A. The information to be searched is described in the following paragraphs and in Attachment B.

4. There is probable cause to believe that certain information, herein described, may be found in the following property: account/s where your affiant believes evidence may be located relating to criminal violations of: Title 18, United States Code, Sections 2252 and 2252A (distribution, receipt and possession of child pornography).

5. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from other agents and witnesses.

6. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Dropbox, Inc. to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the listed accounts, including stored content and the contents of communications. In my training and experience, and based on conversations with other law



enforcement personnel, I have learned that Dropbox, Inc. is an online storage medium on the internet accessed from a computer or electronic storage device. I am aware that computers located at Dropbox, Inc. contain information and other stored electronic communications belonging to unrelated third parties. Accordingly, this affidavit and application for search warrant seeks authorization solely to search the accounts listed in Attachment A by following the procedures described herein and in Attachment B.

7. Because this affidavit is being submitted for the limited purpose of securing the requested search warrant, this affidavit does not purport to set forth all of the facts and circumstances known to me about this matter. Instead, this affidavit sets forth only those facts that I believe are necessary to establish probable cause to believe that evidence of violations of Title 18, United States Code, Sections 2252, 2252A (distribution, receipt and possession of child pornography), will be found on or in the subject property / premises listed above.

**BACKGROUND REGARDING COMPUTERS, THE INTERNET, AND E-MAIL**

8. The term computers as used herein is defined in 18 U.S.C. §1030(e)(1), and includes an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

9. I have had both training and experience in the investigation of computer-related crimes and I have also discussed such crimes, and the investigation of such crimes, with other law enforcement agents. Based on my training, experience and knowledge, and my discussions with other law enforcement agents, I know the following:

10. The Internet is a worldwide network of computer systems operated by governmental entities, corporations and universities. In order to access the Internet, an individual

computer user must subscribe to an Internet Service Provider (ISP), which operates a host computer system with direct access to the Internet. The world wide web (www) is a functionality of the Internet which allows users of the Internet to share information;

11. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any means, including modem, local area network, wireless and numerous other methods;

12. E-mail is a popular form of transmitting messages and/or files in an electronic environment between computer users. When an individual computer user sends e-mail, it is initiated at the user's computer, transmitted to the subscriber's mail server, then transmitted to its final destination. A server is a computer that is attached to a dedicated network and serves many users. An e-mail server may allow users to post and read messages and to communicate via electronic means.

#### **BACKGROUND ON COLLECTORS OF CHILD PORNOGRAPHY**

13. Individuals who are interested in child pornography may want to keep the child pornography files they receive for use in the future. Individuals who collect child pornography may go to great lengths to conceal and protect from discovery their collections of illicit materials. They often maintain their collections in the privacy and security of their homes or other secure location.

14. Individuals who collect child pornography may seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. This contact also may help these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet-based vehicles used by such individuals to communicate with

each other include, but are not limited to, mail, email groups, bulletin boards, IRC, newsgroups, instant messaging, and other similar vehicles.

15. Individuals who collect child pornography may maintain stories, books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children, as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals may keep these materials because of the psychological support they provide.

16. Individuals who collect child pornography may keep names, e-mail addresses, phone numbers or lists of persons who have shared, advertised or otherwise made known their interest in child pornography or sexual activity with children. These contacts may be maintained as a means of personal referral, exchange or commercial profit. This information may be maintained in the original medium from which it was derived, in lists, telephone or address, on computer storage devices, or merely on paper.

### **PROBABLE CAUSE**

17. On March 24, 2017, New York State Police Investigator Hudson adopted an investigation from a cyber-tip in which Dropbox reported that three (3) video files consistent with child pornography were uploaded to Dropbox account “heavyfoot48@hotmail.com,” with screen name “Mark Wall.” A Dropbox upload log was provided with the cyber-tip, which showed that the three (3) files were uploaded on 12/04/2015. Dropbox also provided a login IP for the account of 172.77.34.21 on 09/04/16 at 9:54:41 UTC and assigned to Frontier Communications.

18. On April 3, 2017, the State of New York, Office of Attorney General, issued a Subpoena to Frontier Communications for IP address 172.77.34.21 on 09/04/2016 at 09:54:41UTC and to Dropbox for account heavyfoot48@hotmail.com. On April 4, 2017, Frontier

Communications provided subscriber information for IP 172.77.34.21 in the name of a female with the initials “P.P.” residing on Kibby Road, Lysander, NY. Frontier Communications indicated that the length of service had been from 3/8/16 to present.

19. On May 15, 2017, a subpoena response from Dropbox provided no further information.

20. On June 5, 2017, your affiant began to assist New York State Police Investigator Harrington in the investigation, and we reviewed together the case and three (3) videos that were included in the Dropbox cyber-tip. The videos are available for the Court’s inspection upon request, and are described as follows:

- a. **03ee6dac-81b7-4a0c-bcd4-057424d7173b (1).mp4**, uploaded at 12/04/15 at 3:08pm, is a file comprising three video clips. The first shows a prepubescent juvenile female approximately 12 years of age, wearing pants and socks, dancing while removing clothes in front of the camera. The second and third clips show the juvenile exposing her vagina in lewd and lascivious manner and inserting foreign objects into her vagina.
- b. **71429c2f-fd52-4803-a050-f81c36b60284.mp4**, uploaded on 12/04/15 at 03:10pm, depicts an adult male’s erect penis penetrating a prepubescent female’s vagina.
- c. **b9beab9a-1291-40eb-8995-4b3cdb599428.mp4**, uploaded on 12/04/15 at 03:08pm, depicts a juvenile female removing her clothes while dancing in front of a camera, eventually exposing her vagina and breasts in a lewd and lascivious manner.

21. On June 5, 2017, a query on Spokeo, an open-source internet search tool, revealed the email address heavyfoot48@hotmail.com is associated with Mark Wallace, Kibby Rd., Baldwinsville, NY. This is the same road provided on the Frontier subpoena return. The Dropbox username of “Mark Wall” is also consistent with WALLACE being the user of the account.

22. On June 8, 2017, your affiant and NYSP Investigator Harrington attempted to interview WALLACE at his place of employment. At approximately 8:30am, we met with WALLACE and advised him that law enforcement was conducting an investigation relating to Dropbox and the transmission of images of child pornography. WALLACE consented to an interview and for law enforcement to view his phone. WALLACE was then transported to the New York State Police barracks, located in Lysander, NY. At approximately 08:44am, WALLACE waived his right to counsel and agreed to an interview which was audio and video recorded.

23. During the interview, WALLACE admitted to receiving and viewing child pornography. WALLACE stated he first saw child pornography about two to three years ago. WALLACE said he would have sexually-related chats with people on the Kik mobile social media application. WALLACE stated that during one of these chats, someone sent him child pornography -- either as a link to Dropbox that contained child pornography or by sending him pictures or videos of child pornography in the Kik app. WALLACE further stated that he understood child pornography as pictures and videos of kids involved in sexual acts, either with each other or adults. WALLACE stated that although he did not search for the child pornography the first time, it interested him, and he became sexually aroused by it. WALLACE stated that since then he has continued to chat with more people who would send him child pornography, always over the Kik app.

24. WALLACE further stated during the interview that his Kik username is "Drumgod48." He stated that when people send him pictures or links on Kik, he sometimes saves them to his Dropbox account or on his phone's gallery. WALLACE admitted to using the Dropbox account heavyfoot48@hotmail.com, until it was "shut down." WALLACE stated he now uses the

Dropbox account heavyfoot48@gmail.com. WALLACE said he currently has child pornography pictures and videos on his cell phone and in his Dropbox account.

25. WALLACE also provided oral and written consent to view his phones and social media accounts to include Dropbox and Kik. Your affiant then previewed WALLACE's phone, which is a Samsung Galaxy, model number SM-J327P, serial number 352510088975760. Your affiant observed WALLACE's Kik account Drumgod48. Within this account, your affiant observed chat communication between a Kik account user (hereinafter "Individual A") and WALLACE's account Drumgod48. During the communication, Individual A stated that he spies on his 13 year-old daughter and posts a nude picture of a juvenile female changing. WALLACE then asked if he could see the youngest pictures Individual A has of the daughter. WALLACE also asked for pictures and videos of young boys. Individual A then states he has a 5 year old nephew and 3 year old niece and that they are too young to know if they are being touched. Individual A then stated that in the pictures he is penetrating the boy with his finger and rubbing his penis on the boy's anus. WALLACE asked for these pictures and when he receives them, comments: "That's ok have one of his cock too?" "nice," "I like that," "wish you had vids," "your inside him, Im sure that's nice and tight." Individual A then stated that he has sexual contact with his niece and describes how he engages in oral and vaginal sex with her. WALLACE responded, "wish I could see that" and "wish you had vids." WALLACE then received several images of a nude toddler's vagina being manipulated by an adult male hand. Your affiant then ended the preview of the Kik chat.

26. Your affiant then located the Dropbox account heavyfoot48@gmail.com within the Samsung Galaxy cellphone, which contained hundreds of images and video files. Within these files your affiant observed an image file depicting a juvenile prepubescent girl lying naked, pulling

her legs back, exposing her vagina in a lewd and lascivious manner. Your affiant then ended the preview and located the gallery file located on the Samsung Galaxy. Your affiant observed several images of child pornography, saved and located within a gallery folder. These images were those that WALLACE received from Individual A in the aforementioned Kik chat dialogue.

**DROPBOX**

27. Based on my training and experience, I have learned the following about  
Dropbox, Inc.:

- a. “Dropbox” refers to an online storage medium on the internet accessed from a computer or electronic storage device. As an example, online storage mediums such as Dropbox make it possible for the user to have access to saved files without the requirement of storing said files on their own computer or other electronic storage device. Dropbox is “offsite” storage medium for data that can be viewed at any time from any device capable of accessing the internet. Users can store their files on Dropbox and avoid having the files appear on their computer. Anyone searching an individual’s computer that utilizes Dropbox would not be able to view these files if the user opted only to store them at an offsite such as Dropbox.
- b. Dropbox provides a variety of online services, including online storage access, to the general public. Dropbox allows subscribers to obtain accounts at the domain name [www.dropbox.com](http://www.dropbox.com). Subscribers obtain a Dropbox account by registering with an email address. During the registration process, Dropbox asks subscribers to provide basic personal identifying information. This information can include the subscriber’s full name, physical address, telephone numbers and other identifiers,

alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

- c. When the subscriber transfers a file to a Dropbox account, it is initiated at the user's computer, transferred via the internet to the Dropbox servers, and then can automatically be synchronized and transmitted to other computers or electronic devices that have been registered with that Dropbox account. This includes online storage in Dropbox servers. If the subscriber does not delete the content, the files can remain on Dropbox servers indefinitely. Even if the subscriber deletes their account, it may continue to be available on the Dropbox servers for a certain period of time.
- d. Online storage providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, online storage providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.
- e. In some cases, Dropbox account users will communicate directly with Dropbox about issues relating to the account, such as technical problems, billing inquiries,



or complaints from other users. Online storage providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. To sign into the user's Dropbox account, the user enters an email and password. Once a user has a Dropbox account, they can invite other Dropbox users to access their shared folders. A shared folder is one in which more than one user has access to, and can add, download or delete content.

### **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

28. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Dropbox, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B. These persons will include not only federal law enforcement agents, but also any members of any other state or local law enforcement agency requested to assist in this investigation.

### **CONCLUSION**

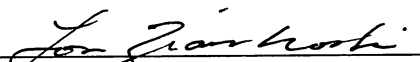
29. Based upon the above information, I believe probable cause exists that there have been violations of Title 18, United States Code, Sections 2252 and 2252A (distribution, receipt and possession of child pornography), and that there is probable cause to believe that information, which is stored at premises owned, maintained, controlled, or operated by: Dropbox, Inc.,

headquartered at 185 Berry Street, 4th Floor, San Francisco, CA 94107 in accounts that will provide evidence of these violations.

30. In consideration of the foregoing, I respectfully request that this Court issue a search warrant to Dropbox, Inc., authorizing the disclosure of the information requested in the enclosed attachments.

31. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

32. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

  
Lon Ziankoski, Special Agent  
Department of Homeland Security

Sworn and subscribed to before me  
this 9th day of June, 2017.

  
HON. DAVID E. PEEBLES  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

**Property to be searched**

The property to be searched are the Dropbox accounts associated with Mark J. Wallace, Jr., heavyfoot48@hotmail.com, heavyfoot48@gmail.com and/or the screen name “Mark Wall” that are stored at premises owned, maintained, controlled, or operated by Dropbox, Inc., headquartered at 185 Berry Street, 4th Floor, San Francisco, CA 94107 (hereinafter, the “accounts”).

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Dropbox, Inc.**

To the extent that the information described in Attachment A is within the possession, custody, or control of Dropbox, Inc. including any messages, records, files, images/videos, logs, contacts or information that have been deleted but are still available to Dropbox, Inc. or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Dropbox, Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all communications associated with the listed accounts, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
- b. All records or other information regarding the identification of the accounts, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the accounts were created, the length of service, the IP address used to register each account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;

d. All records or other information stored at any time by an individual using the accounts, including address books, contact and buddy lists, calendar data, pictures, documents and files;

e. All records pertaining to communications between Dropbox and any person regarding the account, including contacts with support services and records of actions taken; and

f. All connection logs and records of user activity for the account, including:

- i. Connection and date time;
- ii. Disconnect date and time;
- iii. Method of connection;
- iv. Data transfer volume;
- v. User name associated with the connection and other connection information, including the internet protocol address of the source of the connection; and
- vi. Connection information for other computers to which the user of the above-referenced accounts connected, by any means, during the connection period, including the destination IP address, connection time and date, disconnect time and date, method of connection to the destination computer, the identities (account and screen names) and subscriber information, if known, for any person or entity to which such connection information relates, and all other information related to the connection from ISP or its subsidiaries.

## **II. Information to be seized by the government**

All information described above in Section I that constitutes evidence and instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A (distribution, receipt and possession of child pornography), from January 1, 2014 to present, including, for each account or identifier listed on Attachment A:

- (a) Subscriber information, such as name, email address, zip code and other personal/biographical information;
- (b) Account access information, master and sub account names, user profiles, friends lists, instant messages, grief reports, account creation information, associated IP information for each account use, screen shots of account activity, email transaction information;
- (c) Computer records and evidence identifying who the particular user was who received, downloaded, possessed, or accessed with intent to view any child pornography found on any computer or computer media (evidence of attribution), or who attempted to do any of the foregoing, and how the computer was used to effectuate that activity;
- (d) Any and all visual depictions of minors, including, but not limited to, sexually explicit images of minors.
- (e) Any and all chats, chat logs, emails, and other text documents, describing or relating to sexually explicit conduct with children, as well as fantasy writings regarding, describing, or showing a sexual interest in children.

- (f) Any and all address books, names, and lists of names and addresses of minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18 United States Code, Section 2256(2).
- (g) Any and all notebooks and any other records reflecting personal contact, and any other activities, with minors who may be visually depicted while engaged in sexually explicit conduct, or engaged in sexually explicit chat, email, or other communications.
- (h) Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, notes, and sexual aids.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC  
BUSINESS RECORDS PURSUANT TO FEDERAL RULE  
OF EVIDENCE 902(11)**

I, \_\_\_\_\_, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Dropbox and my official title is \_\_\_\_\_. I am a custodian of records for Dropbox. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Dropbox and that I am the custodian of the attached records. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Dropbox; and

c. such records were made by Dropbox as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature